CLAIMS:

1. A system for communicating data and protecting rights therein, comprising:

at least one user device for receiving data;

a server in communication with said at least one user device and including a trusted lock;

a rights management engine for determining user rights in said data;

a storage device for storing said data; and

a storage device for recording an audit trail.

2. A system according to claim 1, wherein said server, rights management engine, data storage and audit trail storage are in a secure location separate from the user device so that trusted services including trusted timing, auditing and copying are performed in a secure environment.

3. The system according to claim 1, wherein said user device includes a storage device for holding data which is released under instructions from said server.

4. The system according to claim 1, wherein said server and user device are connected through a wireless connection.

5. The system according to claim 4, wherein said wireless connection is an “always on” connection.

6. A method of communicating data from a server to a user device and protecting rights therein, comprising:

authenticating identification of said server and said user device;

requesting data to be communicated;

authorizing said data to be communicated based on rights attributed to said user device;

recording said authorization to provide for billing information and an audit trail;

communicating said data to said user device.

7. The method according to claim 6, wherein said data is communicated to said user device and stored therein and rendered in sections according to instructions communicated from said server.

8. The method according to claim 6, wherein communication between said server and said user device is a wireless communication.

9. The method according to claim 8, wherein said wireless communication is an "always on" connection.

10. The method according to claim 6, wherein said authorization step is performed by a digital rights management engine in communication with said server.

11. The method according to claim 6, wherein said recording step is performed in a storage device to record authorization along with time and other information in order to provide a trusted audit trail, which is based on trusted time and a trusted third party to sign the recording.

12. The method according to claim 6, wherein said data is originally stored in a content storage device connected to said server.

13. A rights secure communication device for providing data to a user device comprising:

a server;

a data storage device connected to said server for storing said data; and

a digital rights management engine connected to said server for determining rights attributed to users.

14. The communication device according to claim 13, further comprising a secure storage device for recording authorization of data communication in a secure audit trail.

15. The communication device according to claim 13, wherein data is sent from said server to a user through a wireless communication system.

16. The communication device according to claim 15, wherein said wireless communication system is a "always on" connection.

17. A mobile terminal system for receiving protected data, comprising:

a wireless connection including a transmitter and receiver for communicating with a server which stores protected data, stores data relating to rights to use said protected data and the storage device for recording transactions relating to said protected data;

a decryption engine for decrypting encrypted data sent from said server through said wireless connection;

a display device for displaying said protected data to a user of said mobile terminal.

18. The method according to claim 17, wherein said mobile terminal includes a data storage device for temporarily storing protected data.

19. A computer program embodied on a computer readable medium and executable by a computer to communicate data having protected rights, comprising:

communicating wirelessly with a mobile terminal controlled by a user;

determining rights of said user in protected data using a rights management engine;

recording an audit trail of communications with said mobile terminal in a storage device.

20. A computer program according to claim 19, further comprising storing said protected data in a secure location separate from said mobile terminal wherein all operations regarding said protected data are performed in a secure environment.